Calendar No. 1006

101ST CONGRESS
2d Session

SENATE

REPORT
101-544

THE COMPUTER ABUSE AMENDMENTS ACT OF 1990

OCTOBER 19 (legislative day, OCTOBER 2), 1990.—Ordered to be printed

Mr. BIDEN, from the Committee on the Judiciary, submitted the following

REPORT

[To accompany S. 2476]

The Committee on the Judiciary, to which was referred the bill (S. 2476) to amend the criminal code to clarify and expand legal prohibitions against computer abuse, having considered the same, reports favorably thereon with an amendment in the nature of a substitute and recommends that the bill do pass.

CONTENTS

		Page
I.	Purpose	1
II.	Legislative history	2
III.	Discussion	5
IV.	Vote of the committee	7
V.	Text of S. 2476	7
VI.	Section-by-section analysis	9
VII.	Cost estimate	11
VIII.	Regulatory impact statement	11
IX.	Changes in existing law	11

I. PURPOSE

The purpose of S. 2476 is to clarify and strengthen the criminal laws against the intentional transmission of destructive computer programs or codes and to provide a civil remedy for certain forms of computer crime. Businesses, industry, researchers and government increasingly rely on computers. In light of rapid developments in computer technology, it is necessary to revise existing laws governing computer security and abuse to ensure that novel forms of computer abuse are prohibited.

49-010

S523-24

II. Legislative History

Innovations in computer technology continue at a rapid rate. The Computer Abuse Amendments Act of 1990 is the most recent legislation to take on the challenge of keeping our computer crime laws up to date. As Senator Leahy said in introducing S. 2476:

> Technology is hurling us into the 21st century at speeds that leave lawmakers gasping. This bill catches up with some problems already out of hand, by strengthening laws against computer abuse, deterring malicious computer hacking, and aiding prosecution of computer crimes without criminalizing creative attempts at legitimate experimentation.

Congress passed the Computer Fraud and Abuse Act as part of the Comprehensive Crime Control Act of 1984, Public Law 98–473. That was the first law to address computer crime with a specific statute. Prior to that law, prosecutors used the mail and wire fraud statutes (18 U.S.C. 1341 and 1343) to prosecute crimes of computer abuse. The Computer Fraud and Abuse Act of 1984 prohibited unauthorized access to certain categories of computers if the defendant realized monetary gain or obtained access to classified material.

The Computer Fraud and Abuse Act of 1986, Public Law 99–474, clarified and expanded the existing statute. The new prohibitions outlawed fraud using computers and the destruction or alteration of data in computers without authorization. The new offenses, however, were limited to "Federal interest computers." The statute defined that term to mean computers used by financial institutions or the federal government, or one of two or more computers located in different States that are used to commit the offense.

Congress also passed the Electronic Communications Privacy Act (ECPA), Public Law 99–508, in 1986. That law updated the Federal wiretap statute to protect the privacy and security of information transmitted through new computer and telecommunications technologies. The statute addresses the interception of wire, oral and electronic communications, the unauthorized access to stored wire and electronic communications and the use of pen registers and trap and trace devices. ECPA protects the privacy of personal and proprietary information, while satisfying the Government's legitimate law enforcement needs.

In the 101st Congress, the Subcommittee on Technology and the Law held a hearing to explore the threat to computers and the information stored in them posed by new forms of computer abuse, such as computer "viruses" and "worms." On May 15, 1989, the subcommittee heard testimony from FBI Director William S. Sessions and Dr. Clifford Stoll of the Harvard-Smithsonian Center for Astrophysics. Director Sessions, who was accompanied by two of his experts, William A. Bayse, Assistant Director of Technical Services Division, and Kenneth Walton, Deputy Assistant Director of the Criminal Investigative Division, stressed the seriousness of the threat posed by computer viruses and other techniques. He also testified that the Bureau was actively pursuing computer crime and keeping pace with the changes in the technology. He observed that,

while it is appropriate for the bureau to investigate criminal activity vigorously, we must be mindful of the balance between encouraging legitimate experimentation and the free flow of information on the one hand and preventing destructive computer abuse on the other.

Dr. Stoll is an astrophysicist who, while managing the computer system at the Lawrence Berkeley Laboratory, caught a West German spy using computer networks to try to gain access to military information. Dr. Stoll described the crucial importance of computers and computer networks for advanced scientific research. He also emphasized the need for trust and adequate security in those systems. Misuse of computers, whether it is by a spy probing military secrets or by a destructive computer virus or worm released onto a computer network, threatens the work of all computer users.

In response to changes in computer technology and the threat posed by new techniques for creating and transmitting malicious programs and codes, Senators Leahy, Humphrey, and Kohl introduced S. 2476, the Computer Abuse Amendments Act of 1990, on April 19, 1990. The legislation amends the Computer Fraud and Abuse Act of 1986, 18 U.S.C. 1030, to strengthen and clarify the application of Federal law to newly discovered forms of computer abuse. The bill also creates a civil cause of action for violations of the act. Senator Humphrey pointed out, in his statement when S. 2476 was introduced:

> The national and international computer networks which allow the rapid exchange of information and ideas provide one of the great benefits of modern computer technology. But they also provide a window of vulnerability that can be exploited by those who seek to abuse and undermine our computer systems.

On July 31, 1990, the Subcommittee on Technology and the Law held a hearing on S. 2476. Testifying at the hearing were: Deputy Assistant Attorney General Mark Richard; John L. Pickitt, president of the Computer and Business Equipment Manufacturers Association; David R. Johnson, of Wilmer, Cutler & Pickering, Washington, DC; Douglas Jerger, of ADAPSO, the Computer Software and Services Industry Association; and Marc Rotenberg, of Computer Professionals for Social Responsibility.

In his opening statement, Senator Leahy noted that S. 2476 tightens up the laws against computer abuse. It strengthens existing felony provisions for international computer crimes, while establishing a new misdemeanor provision for violations based on reckless conduct. As Senator Leahy stated, "S. 2476 is designed to balance clear punishment for destructive conduct without stifling creative experimentation." Senator Humphrey further noted in his opening statement at the hearing:

> The broader solution [to the problem of computer abuse] lies in the development and implementation of more effective computer security systems and technology. But in the meantime, it is important that we update our computer

crime laws to stay abreast of the rapid changes in computer abuse techniques.

Deputy Assistant Attorney General Richard testified that the laws against computer abuse could be strengthened in a number of ways:

> Overall, existing criminal statutes provide an adequate framework for the prosecution of most types of computer-related criminal conduct. Existing fraud, embezzlement, theft, and destruction of property statutes can be used to punish those who commit these types of offenses with the assistance of a computer. However, as computer criminals become more sophisticated, using viruses, worms and other types of computer software and hardware to commit heretofore unanticipated offenses, the criminal code must be readjusted to keep up with these developments. S. 2476 provides a useful improvement over, and clarification of, the scope of the existing law.

He also discussed the administration's proposal to rewrite the Computer Fraud and Abuse Act. Several of the provisions in the proposal were similar to S. 2476, such as the creation of a misdemeanor for recklessly causing harm with a computer. The sponsors later adopted a number of the administration's suggestions in a Leahy-Humphrey-Kohl substitute amendment.

Mr. Pickitt testified in favor of S. 2476, as balancing the need for strict penalties for criminal conduct with the promotion of innovation and the free flow of information. He stressed that the narrow approach of S. 2476 was preferable to more sweeping legislation:

> We in the computer industry have had great reservations about legislating in this area. Our main concern was that efforts might be made to criminalize certain technologies, rather than the behavior of the individuals who create computer viruses and other harmful computer security threats. The goal of federal computer crime statutes should be to counter criminal behavior and not to inhibit advanced computing techniques. The Leahy-Humphrey bill is narrowly drawn and focuses on criminal behavior.

Messrs. Jerger and Johnson also testified in favor of S. 2476, and provided the Technology Subcommittee with technical suggestions. Many of these suggestions were adopted in the Leahy-Humphrey-Kohl substitute amendment. Mr. Johnson also noted that the administration's more sweeping proposal "may be a broader step than is necessary at this point."

Mr. Rotenberg testified in favor of the creation of the recklessness misdemeanor is S. 2476, observing that it would provide prosecutors with greater flexibility in bringing cases and send a clear message to computer users that they may not engage in computer experiments that put others at risk.

Mr. Rotenberg noted that Computer Professionals for Social Responsibility opposed the expansion in jurisdiction to computers used in interstate commerce or communication. Under questioning from Senator Leahy, Messrs. Pickitt, Johnson, and Jerger agreed that interstate jurisdiction is appropriate, given the interstate

nature of computer networks. Mr. Jerger also noted ADAPSO's support for interstate jurisdiction in his testimony:

> In particular, we applaud the approach of S. 2476 based upon general principles of interstate commerce, rather than the narrower concept of a "Federal interest computer" under present law. We think it should be possible using Federal law, therefore, to prosecute a disgruntled employee who introduces a harmful program code by means other than telecommunications from outside the State where the employer is.

Mr. Rotenberg expressed concern about possible civil liberties violations in current investigations into computer crime, and cautioned against abuse of the new authority created by S. 2476.

Based on the testimony from the July 31, 1990, hearing, the Technology Subcommittee drafted an amendment in the nature of a substitute, implementing many of the suggestions proposed.

The Technology and the Law Subcommittee agreed to a poll of S. 2476 on September 28, 1990, agreed to the Leahy-Humphrey-Kohl amendment in the nature of a substitute and reported the bill favorably, as amended. The Judiciary Committee, at its executive meeting October 4, 1990, favorably reported S. 2476, as amended by the Technology Subcommittee, to the full Senate.

III. Discussion

S. 2476 updates the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. 1030. It addresses changes in computer technology, particularly new computer abuse techniques such as computer viruses and worms, which make prosecutions difficult in some types of cases. S. 2476 clarifies the intent standards and the actions prohibited. These changes will benefit both computer users and law enforcement.

The maintenance of the security and intergrity of computer systems has become increasingly critical to interstate and foreign commerce, communications, education, science, technology and national security. As Senator Leahy observed at the opening of the May 15, 1989 hearing:

> As we move into the hi-tech age, we become increasingly reliant on computers for research, communications, and data storage and retrieval. Research is collaborative—just look at how discoveries were made in superconductivity. As a nation, we cannot afford data that scientists cannot trust. We cannot afford to have scientists refusing to use computer networks to share their discoveries, and thus, advance technology.

The deliberate abuse of computers and computer systems to cause damage, disruption and interference with the functioning of computer systems has already posed significant burdens on numerous computer users. For example, Dr. Stoll described at the May 15, 1989, hearing how his research was halted when Robert Morris, Jr., introduced a computer "worm" on to the INTERNET computer network in November 1988. The program quickly replicated itself and spread to computers throughout the network. It clogged the

network for 2 days, preventing many researchers from using their computers.

The problem knows no national boundaries. Hackers from Australia have been tracked down and arrested for fouling Dr. Stoll's computers here in the United States. This incident was apparently in retaliation for Dr. Stoll's outspokenness on computer security. Sophisticated new computer abuse techniques could also create significant problems for national security. For example, a destructive virus, programmed to destroy data, was planted at Hebrew University in Jerusalem. This incident has been attributed to terrorist activity. Peter Denning, "The Science of Computing: Computer Viruses," American Scientist Vol. 76 (May–June 1988), p. 236.

Other computer problems, using the same kinds of computer programs, have been inadvertent. In December 1989, the Vermont State computer network froze. It was impossible to sign on to the system. Rather than a virus or sabotage, it turned out to be a security device in the form of a "time bomb," built into the system's hardware to deter outside access. The manufacturer of the software had failed to inform the State that a special code would be triggered after a given date, locking out access through normal channels. It was a nuisance to be sure, but certainly without criminal intent.

S. 2476 creates a structure for treating such incidents—whether they are malicious, accidental or reckless—with appropriately balanced legal sanctions.

The bill broadens jurisdiction for newly created sections of the Computer Fraud and Abuse Act, to cover all computers used in interstate commerce or communications. It is the intent of the legislation to exercise the full extent to the powers of Congress under the commerce clause of the United States Constitution, art. I, sec. 8, to prohibit forms of computer abuse which arise in connection with, and have a significant effect upon, interstate or foreign commerce.

A primary focus of the legislation is to avoid the complications and ambiguities created by certain language in the current CFAA. Computer abuse crimes under the current statute must be predicated upon the violator's gaining "unauthorized access" to the affected Federal interest computers. However, as demonstrated by several recent computer abuse incidents, the most severe forms of computer damage are often inflicted upon remote computers to which the violator never gained "access" in the commonly understood sense of that term. Instead, those computers are damaged when a malicious program or code is replicated an transmitted to them by other computers infected by the violator's original transmission.

The new subsection 1030(a)(5) of the CFAA created by this act makes it clear that one who transmits a destructive program or code with harmful intent is criminally responsible for the resultant damge to all affected computers, without regard to the element of "unauthorized access." The new provision places the focus on harmful intent and resultant harm, rather than on the technical concept of computer "access."

The bill creates a new, civil remedy for those harmed by violations of the Computer Fraud and Abuse Act. This would boost the deterrence of the statute by allowing aggrieved individuals to

obtain relief. As Senator Metzenbum has pointed out, this remedy is not intended to be used against governmental whistleblowers, who reveal information stored in a computer, for the purpose of exposing wrongdoing.

IV. Vote of the Committee

On October 4, 1990, with a quorum present, by voice vote, the Committee on the Judiciary unanimously ordered the bill, S. 2476, as amended in the Subcommittee on Technology and the Law, favorably reported.

V. Text of S. 2476, as Reported

[101st Cong., 2d Sess.]

A BILL to amend title 18 of the United States Code to clarify and expand legal prohibitions against computer abuse

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Computer Abuse Amendments Act of 1990".

SEC. 2. AMENDMENTS TO THE COMPUTER FRAUD AND ABUSE ACT.

(a) Prohibition.—Section 1030(a)(5) of title 18, United States Code, is amended to read as follows:

"(5)(A) through means of or in a manner affecting a computer used in interstate commerce or communications, knowingly causes the transmission of a program, information, code, or command to a computer or computer system if—

"(i) the person causing the transmission intends that such transmission will—

"(I) damage, or cause damage to, a computer, computer system, network, information, data, or program; or

"(II) withhold or deny, or cause the withholding or denial, of the use of a computer, computer services, system or network, information, data or program; and

"(ii) the transmission of the harmful component of the program, information, code, or command—

"(I) occurred without the knowledge and authorization of the persons or entities who own or are responsible for the computer system receiving the program, information, code, or command; and

"(II)(aa) causes loss or damage to one or more other persons of value aggregating $1,000 or more during any 1-year period; or

"(bb) modifies or impairs, or potentially modifies or impairs, the medical examination, medical diagnosis, medical treatment, or medical care of one or more individuals; or

"(B) through means of or in a manner affecting a computer used in interstate commerce or communication, knowingly

causes the transmission of a program, information, code, or command to a computer or computer system—

"(i) with reckless disregard of a substantial and unjustifiable risk that the transmission will—

"(I) damage, or cause damage to, a computer, computer system, network, information, data or program; or

"(II) withhold or deny or cause the withholding or denial of the use of a computer, computer services, system, network, information, data or program; and

"(ii) if the transmission of the harmful component of the program, information, code, or command—

"(I) occurred without the knowledge and authorization of the persons or entities who own or are responsible for the computer system receiving the program, information, code, or command; and

"(II)(aa) causes loss or damage to one or more other persons of a value aggregating $1,000 or more during any 1-year period; or

"(bb) modifies or impairs, or potentially modifies or impairs, the medical examination, medical diagnosis, medical treatment, or medical care of one or more individuals;".

(b) PENALTY—Section 1030(c) of title 18, United States Code is amended—

(1) in paragraph (2)(B) by striking "and" after the semicolon;

(2) in paragraph (3)(A) by inserting "(A)" after "(a)(5)"; and

(3) in paragraph (3)(B) by striking the period at the end thereof and inserting "; and"; and

(4) by adding at the end thereof the following:

"(4) a fine under this title or imprisonment for not more than 1 year, or both, in the case of an offense under subsection (a)(5)(B).".

(c) CIVIL ACTION.—Section 1030 of title 18, United States Code, is amended by adding at the end thereof the following new subsection:

"(g) Any person who suffers damage or loss by reason of a violation of the section, other than a violation of subsection (a)(5)(B), may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. Damages for violations of any subsection other than subsection (a)(5)(A)(ii)(II)(bb) or (a)(5)(B)(ii)(II)(bb) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage.".

(d) REPORTING REQUIREMENTS.—Section 1030 of title 18 United States Code, is amended by adding at the end thereof the following new subsection:

"(h) The Attorney General shall report to the Congress annually, during the first 3 years following the date of the enactment of this subsection, concerning prosecutions under section 1030(a)(5) of title 18, United States Code.".

(e) DEFINITION.—Section 1030(e)(1) of title 18, United States Code, is amended by striking ", but such term does not include an auto-

mated typewriter or typesetter, a protable hand held calculator, or other similar device".

(f) PROHIBITION.—Section 1030(a)(3) of title 18 United States Code, is amended by inserting "adversely" before "affects the use of the Government's operation of such computer".

VI. SECTION-BY-SECTION ANALYSIS

SECTION 1

This title, when enacted, may be cited as the "Computer Abuse Amendments Act of 1990."

SECTION 2

Subsection (a) would amend subsection (a)(5) of the Computer Fraud and Abuse Act of 1986, 18 U.S.C. 1030. It clarifies the intent standards, the actions prohibited and the jurisdiction of the statute. The amendments would cover all computers involved in interstate commerce, not just "Federal interest computers," as the current law does. This is appropriate because of the interstate nature of computer networks and the ease with which computer abuse, such as destructive computer viruses or worms, can spead across State lines. The legislation retains the jurisdictional threshold of $1,000 worth of damage, except for tampering with medical records, where no dollar amount is required.

The new statutory subsection (a)(5)(A)(i) would prohibit knowingly transmitting or causing to be transmitted a program or computer code, if the perpetrator intends that the program will damage or prevent the use of the affected computer. The new subsection focuses on criminal intent, making it clear that the perpetrator must intend to transmit the code and intend to cause damage. This clarifies the existing felony provision, which prohibits "intentionally access[ing] a Federal interest computer without authorization." 18 U.S.C. 1030(a)(5). The Leahy-Humphrey-Kohl substitute amendment adopts the Justice Department's formulation of the actions that should be prohibited in 18 U.S.C. 1030(a)(5), as a more precise formulation that the original language in the bill.

The new subsection (a)(5)(A)(ii) requires that, in order to be criminal, actions would have to be taken without the authorization of the person responsible for the computer system receiving the program. This would prevent criminal liability for honest mistakes and legitimate experimentation under the guidance of a system manager.

The legislation also would create a misdemeanor, in the new subsection (a)(5)(B), for knowingly transmitting a computer program with reckless disregard of a substantial and unjustifiable risk that the transmission will cause harm. The standard for recklessness used in the bill is taken from the Model Penal Code. The misdemeanor parallels the felony created above in new subsection (a)(5)(A).

Subsection (b) creates penalties for violations of the new felony and misdemeanor, modifying 18 U.S.C. 1030(c). This provision tracks current law for the felony penalty: up to 5 years in prison and/or a fine of up to $250,000. It creates an appropriate penalty

for the misdemeanor: up to 1 year in prison and/or a fine of up to $5,000.

Subsection (c) would create a civil cause of action for those who suffer violations of the Computer Fraud and Abuse Act. Plaintiffs would still have to meet the the $1,000 threshold, except for medical records violations. This remedy would authorize private suits in an area that law enforcement has sometimes been reluctant to investigate or prosecute. Deterrence is another goal. The Leahy-Humphrey-Kohl substitute amendment narrowed the damages available and added a 2-year statute of limitations. Damages are limited to economic damages, except for violations of the medical records section, when pain and suffering damages would be permitted.

Subsection (d) was added in the Leahy-Humphrey-Kohl substitute amendment. It requires the Justice Department to report to Congress annually, for the first 3 years after this legislation is enacted, about prosecutions under the new subsections (a)(5)(A) and (B). This provision will both enable Congress to evalaute the effectiveness of the new law in an area of continually changing technology and provide oversight on the prosecutions brought. The reporting requirement is patterned after the original reporting requirement in the Computer Fraud and Abuse Act of 1984, Public Law 98-473.

Subsection (d) was also added in the substitute amendment. It modifies the definition of "computer" in 18 U.S.C. 1030(e)(1), to eliminate the exclusion of typewriters, typesetters, calculators, and similar hand-held devices from the law's current definition. This change was suggested by the Department of Justice and ADAPSO at the July 31, 1990, hearing. It is important because of changes in technology. Many computers include typesetting functions, and "hand-held devices" could cover some miniaturized computers newly available on the market.

Finally, subsection (f) clarifies that a violation of 18 U.S.C. 1030(a)(3), regarding gaining unauthorized access to Federal Government computers, occurs only if the unauthorized access adversely affects the Government's use of the computer. Merely signing on to a Government computer can "affect" the Government's use of the computer, without causing harm.

In addition to these additions, the Leahy-Humphrey-Kohl substitute also eliminated the definition of the term "access" that was in the original bill. "Access" is used throughout the Computer Fraud and Abuse Act, although it is not employed in the sections created by S. 2476. After lengthy consultation with experts in the computer field, the Technology Subcommittee determined that defining the term may cause additional difficulties for prosecutors, since the technology involved is in a constant state of change. The committee believes that the courts should interpret the term "access" with a view to enforcing the overall intent of the CFAA and this supplemental legislation.

VII. Cost Estimate

U.S. Congress,
Congressional Budget Office,
Washington, DC, October 12, 1990.

Hon. Joseph R. Biden, Jr.,
Chairman, Committee on the Judiciary,
U.S. Senate, Washington, DC.

Dear Mr. Chairman: The Congressional Budget Office has reviewed S. 2476, the Computer Abuse Amendments Act of 1990, as ordered reported by the Senate Committee on the Judiciary on October 4, 1990.

S. 2476 would amend and expand federal laws dealing with computer fraud and abuse. The bill would expand current law to cover all computers involved in interstate commerce, not just federal interest computers. S. 2476 also would create a misdemeanor offense for reckless harm; current law addresses only intentional harm, which is a felony. In addition, the bill would create a civil cause of action for those harmed by a violation of the 1986 Computer Fraud and Abuse Act.

Based on information from the Departments of Justice and the Treasury, CBO estimates the enactment of S. 2476 would result in no significant cost to the federal government. There would be additional investigations and prosecutions associated with enactment of S. 2476, but CBO does not expect that the costs associated with the additional activities would be significant.

No costs would be incurred by state or local governments as a result of enactment of this bill.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Mitchell Rosenfeld, who can be reached at 226-2860.

Sincerely,

Robert F. Hale
(For Robert D. Reischauer).

VIII. Regulatory Impact Statement

Pursuant to paragraph 11(b), Rule XXVI of the Standing Rules of the Senate, the Judiciary Committee, after due consideration, concludes that the bill, S. 2476, will not have direct regulatory impact.

IX. Changes in Existing Law

In compliance with paragraph 12 of rule XXVI of the Standing Rules of the Senate, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets; new matter is printed in italic; existing law in which no change is proposed is shown in roman):

Title 18—Crimes and Criminal Procedure

* * * * * * *

CHAPTER 47—FRAUD AND FALSE STATEMENTS

* * * * * * *

§ 1030. Fraud and related activity in connection with computers

(a) Whoever—

(1) knowingly accesses a computer without authorization or exceeds authorized access, and by means of such conduct obtains information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph r. of section 11 of the Atomic Energy Act of 1954, with the intent or reason to believe that such information so obtained is to be used to the injury of the United States, or to the advantage of any foreign nation;

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(3) intentionally, without authorization to access any computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct *adversely* affects the use of the Government's operation of such computer;

(4) knowingly and with intent to defraud, accesses a Federal interest computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer;

[(5) intentionally accesses a Federal interest computer without authorization, and by means of one or more instances of such conduct alters, damages, or destroys information in any such Federal interest computer, or prevents authorized use of any such computer or information, and thereby—

[(A) causes loss to one or more others of a value aggregating $1,000 or more during any one year period; or

[(B) modifies or impairs, or potentially modifies or impairs, the medical examination, medical diagnosis, medical treatment, or medical care of one or more individuals or]

(5)(A) through means of or in a manner affecting a computer used in interstate commerce or communications, knowingly causes the transmission of a program, information, code, or command to a computer or computer system if—

(i) the person causing the transmission intends that such transmission will—

(I) damage, or cause damage to, a computer, computer system, network, information, data, or program; or

(II) withhold or deny, or cause the withhoding or denial, of the use of a computer, computer services, system or network, information, data or program; and

(ii) the transmission of the harmful component of the program, information, code, or command—

(I) occurred without the knowledge and authorization of the persons or entities who own or are responsibilc for the computer system receiving the program, information, code, or command; and

(II)(aa) causes loss or damage to one or more other persons of value aggregating $1,000 or more during any 1-year period; or

(bb) modifies or impairs, or potentially modifies or impairs, the medical examination, medical diagnosis, medical treatment, or medical care of one or more individuals; or

(B) through means of or an in a manner affecting a computer used in interstate commerce or communication, knowingly causes the transmission of a program, information, code, or command to a computer or computer system—

(i) with reckless disregard of a substantial and unjustifiable risk that the transmission will—

(I) damage, or cause damage to, a computer, computer system, network, information, data or program; or

(II) withhold or deny or cause the withholding or denial of the use of a computer, computer services, system, network, information, data or program; and

(ii) if the transmission of the harmful component of the program, information, code, or command—

(I) occurred without the knowledge and authorization of the persons or entities who own or are responsible for the computer system receiving the program, information, code, or command; and

(II)(aa) causes loss or damage to one or more other persons of a value aggregating $1,000 or more during any 1-year period; or

(bb) modifies or impairs, or potentially modifies or impairs, the medical examination, medical diagnosis, medical treatment, or medical care of one or more individuals;

(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if—

(A) such trafficking affects interestate or foreign commerce; or

(B) such computer is used by or for the Government of the United States; shall be punished as provided in subsection (c) of this section.

(b) Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.

(c) The punishment for an offense under subsection (a) or (b) of this section is—

(1)(A) * * *

* * * * * * *

(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; [and]

(3)(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(5) *(A)* of this section which does not occur after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4) or (a)(5) of this section which occurs after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph[.], *and*

(4) a fine under this title or imprisonment for not more than 1 year, or both, in the case of an offense under subsection (a)(5)(B).

(d) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section. Such authority of the United States Secret Service shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.

(e) As used in this section—

(1) the term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device[, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device];

* * * * * * *

(f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.

(g) Any person who suffers damage or loss by reason of a violation of the section, other than a violation of subsection (a)(5)(B), may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. Damages for violations of any subsection other than subsection (a)(5)(A)(ii)(II)(bb) or (a)(5)(B)(ii)(II)(bb) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage.

(h) The Attorney General shall report to the Congress annually, during the first 3 years following the date of the enactment of this subsection, concerning prosecutions under section 1030(a)(5) of title 18, United States Code.

○